## DETAILED ACTION

1. In response to amendment filed on 8 August 2008 and Examiner Initiated Interview on 9 October 2008. Claims 86, 99, and 119, have been amended. Claims 1-85, 87-88, 113-115, and 124, have been cancelled. Amendments to the claims are accepted.

2. An examiner's amendment to the record is attached. Please enter entire claim set. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee. The examiner's amendment was authorized by attorney of record Eric Hiponia in phone interview on 9 October 2008 and confirming email sent on 10 October 2008.

3. The IDS sent on 13 March 2008 and 8 August 2008 has been considered.

### *Response to Arguments*

4. Applicant's arguments filed 8 August 2008 have been fully considered and they are persuasive.

### *Allowable Subject Matter*

5. Claims 86, 89-112, and 116-123, are allowed.

### *Conclusion*

6. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance".

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 7:30 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/ELLEN TRAN/
Primary Examiner, Art Unit 2434
10 October 2008

## Examiner's Amendment

This listing of the claims will replace all prior versions and listings of the claims in the application:

Listing of Claims:

1-85. (Cancelled)

86. (Currently amended) A method for ~~protecting data~~ content protection in an apparatus ~~having an open system architecture~~ comprising:

receiving encrypted data in the apparatus **according to a first encryption protocol wherein the apparatus comprises:**

**an open system architecture configured to allow end users to add or remove hardware components, software modules, or both;**

**a closed subsystem of the apparatus to receive the encrypted data, wherein the closed subsystem does not allow end users to add hardware components or software modules thereto or remove hardware components or software modules therefrom; and**

**combiner circuitry that may add unprotected graphics and audio data to raw data;**

generating raw data in a closed subsystem of the apparatus within the open system architecture, the raw data being generated in the closed subsystem by decrypting the encrypted data and ~~optionally~~ performing additional processing on the encrypted data **wherein the additional processing comprises:**

**decompressing the encrypted data if compressed encrypted data is received;**

**and manipulating the encrypted data for output**;

preventing access to the raw data outside of the closed subsystem;

**adding any applicable unprotected graphics and audio data to the raw data using the combiner circuitry;**

generating protected data in the closed subsystem by re-encrypting the raw data **using a second encryption protocol to generate protected data with any added graphics and audio data;** and

asserting the protected data from the closed subsystem to an external device or system.

87-88. (Cancelled)

89. (Previously presented) The method of claim 86, wherein the apparatus is an entertainment device.

90. (Previously presented) The method of claim 86, wherein the encrypted data comprises digital video data.

91. (Previously presented) The method of claim 90, wherein receiving encrypted data includes reading the digital video data from a disk.

92. (Previously presented) The method of claim 90, wherein the digital video data comprises high-definition digital video data, and wherein re-encrypting the raw data includes re-encrypting the raw data in accordance with the HDCP (High-bandwidth Digital Data Protection) protocol.

93. (Previously presented) The method of claim 86, wherein re-encrypting the raw data includes the use of key data, and further comprising preventing the key data from being disclosed outside of the closed subsystem except to the external device or system.

94. (Previously presented) The method of claim 86, wherein the encrypted data is received from a source external to the apparatus.

95. (Previously presented) The method of claim 94, wherein the source external to the apparatus is the Internet.

96. (Previously presented) The method of claim 86, further comprising generating additional unprotected data and asserting the additional unprotected data to the closed system.

97. (Previously presented) The method of claim 96, further comprising asserting the additional unprotected data from the closed system to the external device or system without encryption.

98. (Previously presented) The method of claim 86, wherein the external device or system comprises a display device.

99. (Currently Amended) An apparatus comprising:

an open system architecture **configured to allow end users to add or remove hardware components, software modules, or both**;

**combiner circuitry that may add unprotected graphics and audio data to raw data;**

a closed subsystem within the open system architecture **wherein the closed subsystem does not allow end users to add hardware components or software modules thereto or**

**remove hardware components or software modules therefrom**, the closed subsystem configured to:

receive encrypted data **according to a first encryption protocol**,

decrypt **and perform additional processing on** the encrypted data to generate raw data **wherein the additional processing comprises:**

**decompressing the encrypted data if compressed encrypted data is received, and**

**manipulating the encrypted data for output**,

**add any applicable unprotected graphics and audio data to the raw data using the combiner circuitry,** and

re-encrypt the raw data to generate protected data **using a second encryption protocol to generate protected data with any added graphics and audio data**,

further wherein the closed system prevent**s**[[ing]] access to the raw data outside of the closed subsystem; and

an output, the closed subsystem to assert the protected data to an external device or system via the output.

100. (Previously presented) The apparatus of claim 99, wherein the protected data comprises encrypted high-definition digital video data.

101. (Previously presented) The apparatus of claim 99, further comprising a second subsystem configured to generate additional unprotected data and to assert the additional unprotected data to the closed subsystem.

102. (Previously presented) The apparatus of claim 101, wherein the additional unprotected data comprises audiovisual data.

103. (Previously presented) The apparatus of claim 101, wherein the additional unprotected data comprises menu information.

104. (Previously presented) The apparatus of claim 101, wherein the closed subsystem is operable in a first mode to assert the protected data to the output and in a second to assert the additional unprotected data to the output.

105. (Previously presented) The apparatus of claim 99, wherein the closed subsystem is operable to re-encrypt the raw data using key data.

106. (Previously presented) The apparatus of claim 105, wherein the closed subsystem is operable to prevent release of the key data outside of the closed subsystem except to the external device or system.

107. (Previously presented) The apparatus of claim 99, wherein the output includes one or more HDMI (Definition Multimedia Interface) compatible links from the apparatus to the external device or system.

108. (Previously presented) The apparatus of claim 99, wherein the closed subsystem comprises an HD-DVD drive configured to decrypt high-definition digital video read from a disk to generate decrypted data, to perform decompression on the decrypted data to generate raw data, and to generate the protected data by re-encrypting the raw data.

109. (Previously presented) The apparatus of claim 99, wherein the closed subsystem is configured to re-encrypt the raw data in accordance with the HDCP (High-bandwidth Digital Data Protection) protocol.

110. (Previously presented) The apparatus of claim 99, wherein the apparatus is configured to communicate bidirectionally with the external device or system to execute an authentication protocol the prior to assertion of the re-encrypted data to the external device or system.

111. (Previously presented) The apparatus of claim 110, wherein the apparatus executing the authentication protocol includes verifying that the external device or system is authorized to receive the protected data and to establish shared secret values for use in encryption and decryption of data.

112. (Previously presented) The apparatus of claim 99, wherein the apparatus is an entertainment device.

113-115. (Cancelled)

116. (Previously presented) The apparatus of claim 101, wherein the closed subsystem is to re-encrypt the raw data using key data, and is to prevent release of the key data outside of the closed subsystem except to the external device or system.

117. (Previously presented) The apparatus of claim 101, wherein the apparatus is configured to communicate bidirectionally with the external device or system to execute an authentication protocol the prior to assertion of the re-encrypted data to the external device or system.

118. (Previously presented) The apparatus of claim 117, wherein the apparatus executing the authentication protocol includes verifying that the external device or system is authorized to receive the protected data and to establish shared secret values for use in encryption and decryption of data.

119. (Currently Amended) A system comprising:

a first apparatus with an open system architecture **configured to allow end users to add or remove hardware components, software modules, or both**, the first apparatus including **combiner circuitry that may add unprotected graphics and audio data to raw data,** a closed subsystem within the open system architecture **wherein the closed subsystem does not allow end users to add hardware components or software modules thereto or remove hardware components or software modules therefrom**, the closed subsystem configured to

receive encrypted content **according to a first encryption protocol**,

decrypt **and perform additional processing on** the encrypted data to generate raw data **wherein the additional processing comprises:**

**decompressing the encrypted data if compressed encrypted data is received, and**

**manipulating the encrypted data for output**,

**add any applicable unprotected graphics and audio data to the raw data using the combiner circuitry,**

re-encrypt the raw content to generate protected content **using a second encryption protocol to generate protected data with any added graphics and audio data**, and

transmit the protected data via an output, the closed system preventing access to the raw content outside of the closed subsystem; and

a second apparatus including an input to receive the protected content and decryption circuitry to generate raw content by decrypting the encrypted video data.

120. (Previously presented) The system of claim 119, wherein the protected content comprises encrypted high-definition digital video data.

121. (Previously presented) The system of claim 120, wherein the second apparatus includes a digital video monitor.

122. (Previously presented) The system of claim 119, wherein the closed subsystem is configured to receive the encrypted content from a remote source.

123. (Previously presented) The system of claim 119, wherein the closed subsystem is further to perform decompression on the decrypted data in the generation of the raw content.

124. (Cancelled)

/ELLEN TRAN/

Primary Examiner, Art Unit 2434